International Journal of Business, Law, and Education
Publisher: IJBLE Scientific Publications Community Inc.
Volume 7, Number 2, 2026
https://ijble.com/index.php/journal/index

Legal Status and Enforceability of Blockchain-Based Smart Contracts as Electronic Agreements under Indonesian Law

Ida Bagus Mahayana Pidada[1] | Made Aditya Pramana Putra[2]
[12] Faculty of Law, Udayana University, Indonesia
Corresponding author: gusademhynp@gmail.com

Abstract
Blockchain-based smart contracts automate the execution of transactions through computer code, but automation alone does not determine whether the resulting arrangement is a legally binding contract. This article examines the legal status and enforceability of blockchain-based smart contracts as electronic agreements under Indonesian law and evaluates how the validity requirements in Article 1320 of the Indonesian Civil Code operate in a pseudonymous, automated, and relatively immutable technological environment. Using doctrinal legal research, the study integrates the Indonesian Civil Code, the Electronic Information and Transactions Law (EIT Law) as amended by Law No. 1 of 2024, Government Regulation No. 71 of 2019, and current financial-sector regulation, supported by comparative analysis of the UNCITRAL Model Law on Automated Contracting, the UK Law Commission's work on smart legal contracts, and relevant European regulatory design. The analysis finds that Indonesian law can recognize a blockchain-based arrangement as an electronic contract when an identifiable agreement is formed through an electronic system and the substantive validity requirements are satisfied. Government Regulation No. 71 of 2019 is particularly significant because Article 46 reproduces the core elements of contractual validity for electronic contracts, while Article 47 requires party identity, transaction terms, cancellation procedures, and choice-of-law provisions. The principal legal uncertainty therefore lies less in basic contractual validity than in attribution of consent and capacity, code-text inconsistency, automated-agent responsibility, coding or oracle errors, reversibility of remedies, and cross-border enforcement. The article recommends targeted, technology-neutral rules and contractual design safeguards rather than assuming that either code alone or a comprehensive blockchain-specific statute can solve these problems.

Keywords: smart contracts; blockchain; electronic contracts; Indonesian contract law; Article 1320; legal certainty; automated contracting

DOI. https://doi.org/10.56442/ijble.v7i2.1558

INTRODUCTION

Blockchain-based smart contracts sit at the intersection of contract doctrine and automated digital performance. The expression “smart contract” is frequently used as if the presence of executable code itself creates a contract. That assumption is too broad. In technical usage, a smart contract can be software deployed on a distributed ledger; in legal usage, a smart legal contract concerns an agreement whose formation or performance is wholly or partly automated. The distinction matters because code may implement an existing legal agreement, constitute only one evidentiary component of an agreement, or operate without the parties intending to create legally enforceable obligations (Mik, 2017; Raskin, 2017; Werbach & Cornell, 2017). Accordingly, the legal inquiry should not begin with the proposition that every smart contract is a contract. It should ask when an automated blockchain arrangement satisfies the requirements that Indonesian law attaches to contractual formation and performance.

The conceptual roots of smart contracting pre-date contemporary blockchains. Szabo (1997) described smart contracts as protocols that formalize and secure relationships through computer networks, while later scholarship emphasized the relationship between legal prose, code, automation, and enforcement (Clack et al., 2016; De Filippi & Wright, 2018). Blockchain architectures added distributed verification and tamper-resistance, making certain forms of automated performance possible without a single centralized transaction processor. These characteristics can reduce some transaction and monitoring costs, but they do not eliminate the need for contract law. Automated execution may reproduce a drafting error, act on inaccurate external data, or perform despite a legally relevant defect in consent, capacity, good faith, or legality (Giancaspro, 2017; Mik, 2022; Sklaroff, 2017).

Indonesian law already contains a layered framework for this inquiry. Article 1320 of the Indonesian Civil Code requires consent, legal capacity, a specific subject matter, and a lawful cause. The Electronic Information and Transactions Law (EIT Law) defines an electronic contract as an agreement made through an electronic system, recognizes electronic information and documents as legal evidence, and expressly adopts the principle of freedom to choose technology or technological neutrality (Republic of Indonesia, 2008/2024, arts. 1(17), 3, 5). Government Regulation No. 71 of 2019 then provides a more operational rule: Article 46 states that an electronic contract is valid when there is party consent, a legally capable or duly authorized legal subject, a specific matter, and a transaction object that does not violate law, morality, or public order (Republic of Indonesia, 2019, art. 46). This provision is highly relevant because it translates the classical validity requirements into the electronic-transaction setting rather than leaving their application wholly implicit.

The principal problem is therefore more precise than a simple claim that Indonesia has a complete “legal vacuum” for smart contracts. There is no general statute that specifically governs blockchain-based smart contracts as a distinct contractual category, but there is an existing body of contract and electronic-transaction law capable of validating many such arrangements. The unresolved questions concern how those rules operate when a wallet address is pseudonymous, acceptance is expressed through a cryptographic action, contractual performance is delegated to code, external facts are supplied through an oracle, and an automated transfer is difficult to reverse after a court later finds a defect in the underlying agreement. Recent Indonesian scholarship has examined consensualism and the expression of will in smart contracts, but the regulatory interaction among Article 1320, the EIT Law, Government Regulation No. 71 of 2019, automated-agent rules, and post-execution remedies requires a more integrated analysis (Ariyanto, 2024).

This article addresses that gap through two research questions. First, under what conditions may a blockchain-based smart contract qualify as a binding electronic agreement under Indonesian law? Second, how should the four validity requirements and related rules on electronic transactions be applied to the distinctive risks of pseudonymity, automation, coding errors, external-data dependence, relative immutability, and cross-border performance? The article contributes to the literature in three ways. It distinguishes smart-contract code from the legally enforceable agreement; it places Government Regulation No. 71 of 2019 at the center of the validity analysis rather than relying only on Article 1320; and it separates formation validity from the later problems of performance, attribution, remedies, and

enforcement. Comparative materials are used functionally, not as sources of Indonesian law, to identify regulatory design options that may strengthen legal certainty without unnecessarily locking legislation to a particular blockchain architecture.

Conceptual and Legal Framework

1. Smart-contract code, smart legal contracts, and automated performance

A legally useful analysis requires conceptual separation between code and agreement. Smart-contract software can execute instructions when specified conditions are satisfied, but legal obligations arise from a recognized source of obligation rather than from computational execution as such. Raskin (2017) treats automation as a defining feature of smart contracting, while Werbach and Cornell (2017) show that the remedial functions of contract law remain important precisely because automated execution cannot resolve every dispute over formation, interpretation, excuse, or remedy. Mik (2017, 2021) goes further by warning that computer code is not a natural substitute for legal language: code is deterministic within its programmed environment, whereas legal standards often depend on context, interpretation, reasonableness, good faith, or other evaluative concepts.

For the purposes of this article, three configurations are distinguished. In a code-only configuration, parties interact primarily through deployed code and on-chain actions. In a hybrid configuration, a natural-language agreement sets out legal terms while code automates selected obligations. In a code-connected configuration, code performs a transaction but the legally relevant agreement may arise from surrounding communications, platform terms, or an off-chain contract. This taxonomy avoids the circular assumption that because a program is called a “smart contract,” it must already satisfy the legal definition of a contract. It also helps determine which source should prevail where coded behavior and the parties' legally expressed intentions diverge (Clack et al., 2016; Giancaspro, 2017).

2. Indonesian contract law and the electronic-transaction framework

Indonesian contract law operates through the general provisions of Book III of the Civil Code, including the principle that agreements validly entered into bind the parties. Article 1320 supplies the central validity requirements, while Articles 1321 and 1337, among others, address defects in consent and unlawful causes or objects. The relevance of those rules is preserved in electronic environments because the EIT Law does not create a separate, self-contained law of contractual validity. Instead, it recognizes electronic forms and transactions while leaving substantive contractual validity to the general law, supplemented by specific electronic-transaction requirements.

Indonesia’s electronic-transaction framework is more extensive than a simple “absence of regulation” characterization suggests. Article 1(17) defines an electronic contract as an agreement made through an electronic system. Article 3 expressly includes the freedom to choose technology or technological neutrality among the governing principles. Article 17 requires good faith in electronic transactions; Article 18(1) provides that electronic transactions embodied in electronic contracts bind the parties; Article 20 addresses electronic offer and acceptance; and Article 21 allocates legal consequences when transactions are conducted directly, through an authorized representative, or through an Electronic Agent (Republic of Indonesia, 2008/2024).

These provisions do not mention blockchain, but their functional language is capable of applying to new electronic architectures.

Government Regulation No. 71 of 2019 is especially important. Article 45 requires good faith, prudence, transparency, accountability, and fairness in electronic transactions. Article 46 sets the validity requirements for electronic contracts, closely corresponding to Article 1320. Article 47 requires electronic contracts directed to Indonesian residents to use Bahasa Indonesia and to contain, at minimum, party identity data, the object and specifications, transaction requirements, price and costs, cancellation procedures, remedies for hidden defects, and a choice-of-law mechanism for transaction settlement. These minimum-content rules create a direct tension with purely pseudonymous or code-only arrangements: a blockchain transaction may be technically executable while failing to provide contractual information that Indonesian regulation expects an electronic contract to contain (Republic of Indonesia, 2019, arts. 45-47).

3. Legal certainty and comparative regulatory benchmarks

Legal certainty is retained as an evaluative concern, but it should not be treated as an independent rule that makes an otherwise invalid smart contract enforceable. Radbruch's well-known account places legal certainty among the fundamental values of law; in the present context, the concept is useful for asking whether parties can reasonably predict the legal consequences of formation, automated performance, error, termination, and dispute resolution (Radbruch, 2006). This framing is more precise than invoking legal certainty as a general justification for either validating or prohibiting a technology.

Comparative materials reinforce a function-based approach. The UK Law Commission (2021) concluded that existing English contract law can generally accommodate smart legal contracts, while recognizing that automation creates specific issues for formation, interpretation, remedies, deeds, and private international law. UNCITRAL's Model Law on Automated Contracting (2024) similarly seeks legal recognition of automation in contract formation and performance without making enforceability depend on a specific technology. The European Union's Data Act, as enacted in 2023, included design requirements for certain smart contracts used to execute data-sharing agreements, including robustness, safe termination, archiving and auditability, access control, and consistency with the underlying agreement (European Parliament & Council, 2023, art. 36). As of August 2026, that Article is the subject of an EU Digital Omnibus proposal that would remove the smart-contract requirements; the provision is therefore used here only as a design benchmark, not as a model that should be transplanted wholesale.

METHOD

This study employs doctrinal legal research. Doctrinal research identifies, organizes, interprets, and evaluates legal rules and principles in order to state the law applicable to a defined legal problem and to expose areas of uncertainty or inconsistency (Hutchinson & Duncan, 2012). The method is appropriate because the research questions concern the legal characterization, validity, and enforceability of automated contractual arrangements rather than the frequency of smart-contract use or the behavior of market participants.

The primary Indonesian legal materials are the Indonesian Civil Code; Law No. 11 of 2008 concerning Electronic Information and Transactions as amended, most recently, by Law No. 1 of 2024; and Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions. Current OJK regulation of digital financial assets and cryptoassets is examined only to determine the sectoral regulatory context, not as a direct source of general contract validity. This distinction is necessary because responsibility for regulating and supervising cryptoasset trading shifted from Bappebti to the Financial Services Authority (OJK) in January 2025, and the current framework is built around OJK Regulation No. 27 of 2024 as amended by OJK Regulation No. 23 of 2025 (Financial Services Authority, 2025).

The analysis proceeds in four stages. First, the article identifies the legal requirements for a valid electronic agreement and maps them against Article 1320. Second, it classifies the legal function of smart-contract code as possible evidence of assent, a performance mechanism, or part of the contractual terms. Third, it tests the legal rules against recurrent technological features: pseudonymous addresses, private-key authorization, automated agents, oracle dependence, coding error, and difficult-to-reverse execution. Fourth, it uses comparative materials from UNCITRAL, the UK Law Commission, and the European Union to evaluate possible regulatory responses. Comparative materials are persuasive rather than binding and are used to identify functions that Indonesian law may need to address.

The study is limited to civil-law questions of contract formation, validity, performance, evidence, remedies, and related private-law uncertainty. It does not attempt to determine the regulatory classification of every token or decentralized-finance product, nor does it address taxation, anti-money-laundering duties, securities regulation, criminal liability, or consumer law in full. It is also non-empirical: it does not measure judicial outcomes or interview users, developers, judges, or regulators. These limitations should be kept in view when drawing policy conclusions.

RESULTS AND DISCUSSION

1. Legal characterization: conditional recognition, not automatic contractual status

The first finding is that Indonesian law provides a credible basis for recognizing blockchain-based smart contracts as electronic agreements, but recognition is conditional rather than automatic. The decisive statutory concept is an “agreement of the parties made through an Electronic System,” not a software label or the use of blockchain itself (Republic of Indonesia, 2008/2024, art. 1(17)). Accordingly, a deployed program that merely performs computational operations is not necessarily an electronic contract. It acquires contractual significance when the surrounding facts establish an agreement and the substantive and electronic-contract requirements are fulfilled.

This conditional-recognition approach is doctrinally more defensible than treating smart-contract code as automatically contractual. The open character of Indonesian contract law and the EIT Law’s technology-neutral principle support the use of new media for contracting; they do not exempt new media from ordinary rules of validity. The legal relationship remains one of obligation governed by the general law of contract, while blockchain supplies technical infrastructure for recording or automating performance. This distinction is consistent with international literature rejecting the

idea that smart contracts displace contract law (Ferreira, 2021; Werbach & Cornell, 2017).

The current sectoral regulation of cryptoassets does not alter that conclusion. Since January 2025, supervision of digital financial assets and cryptoassets has moved to OJK, with OJK Regulation No. 27 of 2024, as amended by OJK Regulation No. 23 of 2025, governing the trading framework (Financial Services Authority, 2025). Those rules are relevant to regulated cryptoasset activities but do not constitute a general civil code for blockchain contracts. The regulatory gap is therefore specific: Indonesia lacks detailed rules for certain smart-contract performance and remedial problems, not a complete absence of rules governing electronic contractual validity.

Table 1. Mapping Indonesian validity requirements to smart-contract risks

Requirement	Principal legal basis	Application to smart contracts	Primary legal risk
Consent	Civil Code art. 1320; EIT Law arts. 18, 20; GR 71/2019 arts. 46, 49	Electronic acceptance, digital signature, wallet action, or use of a system may evidence assent when linked to an identifiable offer and contractual terms.	Cryptographic authorization does not by itself prove legally valid consent; mistake, fraud, coercion, code-text mismatch, or compromised keys may undermine attribution.
Legal capacity / authority	Civil Code art. 1320; GR 71/2019 art. 46(2)(b)	The contracting subject must be legally capable or duly authorized to represent another subject.	A pseudonymous address does not establish age, legal identity, corporate authority, guardianship status, or representative power.
Specific subject matter	Civil Code art. 1320; GR 71/2019 arts. 46-47	Programmed conditions can increase operational precision where the object and triggering conditions are objectively determinable.	Oracles, ambiguous off-chain facts, incomplete specifications, and divergent code/prose can reintroduce uncertainty.
Lawful cause / object	Civil Code arts. 1320, 1337; GR 71/2019 art. 46(2)(d)	Legality is assessed by the object and purpose of the transaction, not by whether the code executes successfully.	Automatic execution may complete an unlawful or otherwise invalid transaction before legal intervention is possible.

Note. The table synthesizes the Indonesian Civil Code, the EIT Law, and Government Regulation No. 71 of 2019. It does not imply that every smart-contract deployment is itself an electronic contract.

2. Consent: electronic assent is legally possible, but attribution remains contestable

Consent is the first point at which technical and legal reasoning can diverge. The EIT Law recognizes electronic formation and provides that, unless otherwise agreed, an electronic transaction occurs when an electronically transmitted offer is received and accepted electronically (Republic of Indonesia, 2008/2024, art. 20). Government Regulation No. 71 of 2019 similarly recognizes acceptance through a statement of approval or, in certain circumstances, through conduct involving acceptance or use of the object (art. 49). These provisions make it unnecessary to insist on a handwritten document as the sole evidence of agreement.

However, a private key, wallet signature, or transaction confirmation should be treated primarily as evidence of control over a credential and of a digital action, not as irrebuttable proof of a legally valid will. A key can be stolen, used by an unauthorized employee, activated under mistake, or associated with a user who did not understand the legal effect of the transaction. The analytical error would be to collapse

authentication into consent. Authentication helps attribute an electronic act; contract doctrine still asks whether the act objectively and legally constitutes assent to sufficiently disclosed terms (Mik, 2021; Ariyanto, 2024).

The risk is particularly acute in code-only arrangements. Users may interact with a deployed function without reading or even having access to a human-readable statement of the transaction's legal terms. Article 47 of Government Regulation No. 71 of 2019 expects an electronic contract directed to Indonesian residents to contain identity and transaction information, cancellation procedures, and a choice-of-law mechanism. For higher-value or legally complex transactions, a defensible design is therefore a hybrid architecture: human-readable terms identify the parties, rights, remedies, governing law, and precedence rules, while the code automates only the functions that can be represented with sufficient precision. This approach also reduces the interpretive problem identified in the literature when natural-language intent and program behavior do not match (Clack et al., 2016; Mik, 2017).

3. Legal capacity and authority: pseudonymity is the strongest validity challenge

Among the four validity requirements, legal capacity creates the clearest structural difficulty for public-blockchain contracting. Government Regulation No. 71 of 2019 does not merely require an electronic act; Article 46 requires the transaction to be performed by a legally capable subject or by a person authorized to represent that subject. A blockchain address, viewed in isolation, normally does not reveal whether the controller is a minor, a person subject to legal restrictions, a corporate officer acting within authority, an agent exceeding a mandate, or an automated system operated for another person.

This does not make public-blockchain contracting legally impossible. It means that technical pseudonymity and legal anonymity should not be treated as equivalents, and that some transactions require an identity or authority layer external to the blockchain. Possible mechanisms include verified electronic identities, qualified certificates, platform-level know-your-customer procedures where legally required, organizational signing policies, or verifiable credentials that establish role or authority without publishing unnecessary personal data. The appropriate mechanism should be proportionate to transaction value, risk, and legal context.

The distinction is doctrinally important because claims of high transactional or cryptographic security do not answer the capacity question. Cryptographic integrity can show that a transaction was authorized by a key; it does not establish the civil status of the person behind the key. Legal certainty therefore depends on linking technical authorization to the legally relevant subject when capacity or representative authority matters.

4. Specific subject matter, code precision, and the oracle problem

Smart contracts can improve precision where obligations are reducible to objectively verifiable conditions. A payment can be triggered by a timestamp, a digitally verifiable transfer, or another machine-readable event. In that limited sense, automation may strengthen certainty about the mechanism of performance. But code precision should not be confused with contractual completeness. Many commercial obligations depend on facts outside the blockchain or on standards such as reasonable efforts, material breach, satisfactory quality, good faith, or force majeure.

Such standards cannot always be reduced to binary code without losing legal meaning (Mik, 2017; Sklaroff, 2017).

Where performance depends on an external data source, an oracle introduces an additional point of failure and trust. The program may execute exactly as written while relying on inaccurate, delayed, manipulated, or legally disputed input. The resulting problem is not simply a software defect; it concerns contractual allocation of data-source risk. A robust agreement should therefore identify the authorized data source, define fallback procedures, specify consequences of conflicting data, and allocate responsibility where the oracle or data provider fails. Without these provisions, the apparent determinacy of a smart contract may mask uncertainty at the boundary between the blockchain and the external world (Mik, 2022).

5. Lawful cause and technology neutrality

The fourth requirement confirms why technology neutrality is legally useful. Article 3 of the EIT Law expressly recognizes freedom to choose technology or technological neutrality, while Article 46 of Government Regulation No. 71 of 2019 asks whether the transaction object violates law, morality, or public order. The legality of the agreement therefore turns on what the parties seek to accomplish and whether mandatory law is respected, not on whether the transaction uses blockchain. A lawful payment, licensing arrangement, logistics transaction, or other commercial exchange does not become unlawful merely because performance is automated.

The converse is equally important: technically flawless execution does not cure an unlawful object or purpose. Code can execute an arrangement that a court would refuse to recognize or enforce. This illustrates the distinction between technical finality and legal validity. A blockchain may record that a transfer occurred, while private law may subsequently require restitution, damages, or another remedy because the underlying agreement was invalid or because performance violated a mandatory rule.

6. Automated agents, coding errors, and responsibility

The EIT Law's rules on Electronic Agents offer a neglected but potentially important analytical bridge. Article 1(8) defines an Electronic Agent as a device within an electronic system that automatically performs an action on electronic information, and Article 21 allocates legal consequences when transactions are carried out through such an agent (Republic of Indonesia, 2008/2024). A smart contract can functionally resemble an Electronic Agent because it automatically performs programmed actions. Nevertheless, the legal classification should not be assumed in every decentralized deployment, especially where no single operator clearly controls the software after deployment.

Where Article 21 applies, its allocation of responsibility is significant: transactions conducted through an Electronic Agent may place legal consequences on the agent's operator, while failures caused by direct third-party interference or user negligence are treated differently. This framework can inform disputes involving coding defects, compromised interfaces, or automated execution. Yet decentralized architectures complicate the identification of the relevant “operator” when code is written by one developer, deployed by another party, governed by token holders, and accessed through a separate user interface.

Article 22 adds another point of tension by requiring certain Electronic Agents to provide a feature allowing users to change information that is still in the transaction process. That rule reflects a legal preference for correctability before completion. By

contrast, some blockchain systems intentionally make post-confirmation changes difficult. The correct legal response is not to describe blockchain as absolutely immutable; rather, legal analysis should recognize that different systems provide different upgrade, pause, proxy, governance, or migration mechanisms. Contractual and regulatory design should focus on whether a legally effective correction or interruption mechanism exists when intervention is justified (Mik, 2022; Sklaroff, 2017).

7. Evidence, termination, remedies, and the divergence between legal and on-chain states

The EIT Law gives electronic information and electronic documents evidentiary status, which means blockchain records can be relevant proof of transaction history, timing, digital actions, and the state of a program (Republic of Indonesia, 2008/2024, art. 5). Their evidentiary strength, however, depends on what proposition is being proved. A ledger can strongly evidence that an address authorized a transaction at a particular time; it may not prove the real-world identity, capacity, intent, or authority of the person controlling that address.

The most difficult remedial issue arises when legal invalidity is discovered after automated execution. Traditional contract law can rescind, terminate, or award remedies, but a completed on-chain transfer may not be technically reversible through the original program. This does not eliminate legal remedies; it changes how they must be implemented. A court may order restitution, damages, transfer of replacement assets, action by a custodian or platform, or other off-chain relief. The central insight is that the legal state and the blockchain state can diverge. Smart-contract design should therefore anticipate dispute outcomes rather than assuming that technical completion will end the legal inquiry (Raskin, 2017; Werbach & Cornell, 2017).

Cross-border disputes add a further layer. Article 18 of the EIT Law permits parties to choose applicable law and a dispute-resolution forum for international electronic transactions. Government Regulation No. 71 of 2019 also expects a choice-of-law provision in electronic contracts. Yet decentralized networks can involve users, developers, validators, interfaces, custodians, and assets in multiple jurisdictions. A clear governing-law and forum clause is therefore not merely boilerplate; it is a practical risk-control mechanism for hybrid smart legal contracts.

8. Regulatory gap and proportionate reform

The analysis supports a narrower and more defensible account of the regulatory gap. Indonesian law already supplies rules for validity, electronic evidence, good faith, electronic offer and acceptance, automated agents, and minimum electronic-contract content. The strongest uncertainties concern the attribution of legally meaningful consent and authority, the status of code relative to natural-language terms, responsibility for software and oracle failure, procedures for interruption and correction, post-execution remedies, and cross-border enforcement. These are real gaps, but they do not necessarily require a comprehensive new statute that treats all smart contracts as a single legal category.

A technology-neutral approach is preferable because smart-contract architectures vary widely and evolve faster than legislation. The UK Law Commission's experience shows that general contract law can remain effective if courts and parties receive targeted guidance on novel issues (Law Commission, 2021). UNCITRAL's Model Law on Automated Contracting likewise demonstrates that legal systems can recognize automated formation and performance without privileging a particular platform

(UNCITRAL, 2024). The former design of Article 36 of the EU Data Act is also instructive at the engineering-policy level: safe termination, auditability, access control, and consistency between code and the underlying agreement are useful safeguards even though the EU is now considering repeal of that provision (European Parliament & Council, 2023).

Table 2. Targeted regulatory and contractual responses

Issue	Existing Indonesian basis	Residual uncertainty	Recommended response
Code vs. legal terms	Civil Code; EIT Law; GR 71/2019	No specific rule determines precedence where code behaves differently from natural-language terms.	Require a clear precedence clause, accessible human-readable terms, versioning, and auditable linkage between terms and deployed code.
Identity, capacity, authority	GR 71/2019 arts. 46-47; EIT Law electronic-signature framework	Public addresses are pseudonymous and may not establish civil capacity or authority.	Use proportionate identity/credential mechanisms for transactions where capacity or representative authority is legally material.
Error / oracle failure	EIT Law arts. 15, 21; general contract and liability rules	Responsibility can be fragmented among developer, deployer, interface operator, oracle provider, and user.	Allocate software, data-source, audit, update, and failure risk expressly; define fallback data and dispute procedures.
Interruption / correction	EIT Law art. 22; GR 71/2019 cancellation information	Some deployments resist modification after execution.	For material transactions, require or contract for pause, stop, upgrade, escrow, or equivalent remedial mechanisms where technically and legally appropriate.
Evidence / auditability	EIT Law art. 5; electronic-system requirements	Ledger evidence may not prove identity, intent, or authority.	Preserve human-readable terms, transaction hashes, versioned code, audit logs, identity evidence, and relevant off-chain records.
Cross-border enforcement	EIT Law art. 18; GR 71/2019 arts. 47, 50	Decentralized components may span multiple jurisdictions.	Specify governing law, forum/arbitration, service mechanisms, and remedial cooperation with custodians or identifiable operators.

Note. "GR 71/2019" refers to Government Regulation No. 71 of 2019. Recommendations are functional safeguards and should be calibrated to transaction type, risk, and sector-specific law.

CONCLUSION

Blockchain-based smart contracts can be legally recognized as electronic agreements under Indonesian law, but their legal status is not generated by blockchain technology itself. The more accurate proposition is conditional: where the facts establish an agreement made through an electronic system and the requirements of consent, legal capacity or authority, a specific subject matter, and a lawful transaction object are satisfied, Indonesian law provides a basis for binding contractual effect. The EIT Law supplies recognition of electronic contracts, electronic evidence, technology neutrality, good faith, electronic offer and acceptance, and automated-agent transactions, while Government Regulation No. 71 of 2019 expressly restates the core validity requirements for electronic contracts.

This framework means that the principal uncertainty is not a total normative vacuum at the stage of formation. The more difficult questions arise from the interaction between legal doctrine and technical architecture: whether a cryptographic

action reflects genuine contractual assent; whether the person behind a pseudonymous address has capacity or authority; whether code accurately represents the parties' agreement; who bears responsibility for coding, interface, or oracle failures; how a transaction can be interrupted or corrected; and how legal remedies operate after technically final execution. The requirement in Government Regulation No. 71 of 2019 that electronic contracts contain identity information, transaction terms, cancellation procedures, and choice-of-law provisions is particularly significant for assessing code-only or anonymous arrangements.

The analysis therefore supports a more precise response to the call for "comprehensive regulation." Indonesia needs greater legal certainty, but a technology-specific statute is not the only—and may not be the most durable—solution. A more proportionate strategy is targeted, technology-neutral guidance or regulation addressing code-to-contract consistency, identity and authority assurance, responsibility for automated agents and external data, auditability, interruption and correction mechanisms, and enforceable dispute-resolution design. Such an approach preserves freedom of contract and technological neutrality while ensuring that automation remains subordinate to legal requirements protecting valid consent, lawful transactions, effective remedies, and accountable contractual performance.

Because this research is doctrinal and non-empirical, future studies should test these conclusions against Indonesian judicial practice, regulated-industry deployments, and interviews with developers, contracting parties, notaries, judges, and regulators. Comparative work should also examine how automated-contracting rules evolve after the 2024 UNCITRAL Model Law and the ongoing European debate over smart-contract regulation. Those inquiries would help determine which uncertainties can be managed through contract drafting and technical standards and which require legislative intervention.

References

Ariyanto, A. (2024). Development of the statement of will and its validity in smart contract. Jurnal Penelitian Hukum De Jure, 24(2), 199-214. https://doi.org/10.30641/dejure.2024.V24.199-214

Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart contract templates: Foundations, design landscape and research directions. arXiv. https://doi.org/10.48550/arXiv.1608.00771

De Filippi, P., & Wright, A. (2018). Blockchain and the law: The rule of code. Harvard University Press.

Durovic, M., & Willett, C. (2023). A legal framework for using smart contracts in consumer contracts: Machines as servants, not masters. The Modern Law Review, 86(6), 1390-1421. https://doi.org/10.1111/1468-2230.12817

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? Telecommunications Policy, 45(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Giancaspro, M. (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective. Computer Law & Security Review, 33(6), 825-835. https://doi.org/10.1016/j.clsr.2017.05.007

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83-119. https://doi.org/10.21153/dlr2012vol17no1art70

Law Commission. (2021). Smart legal contracts: Advice to Government (Law Com No. 401).

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. Law, Innovation and Technology, 9(2), 269-300. https://doi.org/10.1080/17579961.2017.1378468

Mik, E. (2021). Contracts in code? Law, Innovation and Technology, 13(2), 478-509. https://doi.org/10.1080/17579961.2021.1977220

Mik, E. (2022). Smart contracts: Tales of trust and certainty. Technology and Regulation, 2022, 100-112. https://doi.org/10.71265/z0xrj502

Radbruch, G. (2006). Statutory lawlessness and supra-statutory law (1946) (B. L. Paulson & S. L. Paulson, Trans.). Oxford Journal of Legal Studies, 26(1), 1-11. https://doi.org/10.1093/ojls/gqi041

Raskin, M. (2017). The law and legality of smart contracts. Georgetown Law Technology Review, 1(2), 305-341.

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. Information & Communications Technology Law, 26(2), 116-134. https://doi.org/10.1080/13600834.2017.1301036

Sklaroff, J. M. (2017). Smart contracts and the cost of inflexibility. University of Pennsylvania Law Review, 166(1), 263-303.

Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548

United Nations Commission on International Trade Law (UNCITRAL). (2024). UNCITRAL Model Law on Automated Contracting.

Werbach, K., & Cornell, N. (2017). Contracts ex machina. Duke Law Journal, 67(2), 313-382.

Legal and Regulatory Materials

European Parliament & Council. (2023). Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

Financial Services Authority (OJK). (2024/2025). OJK Regulation No. 27 of 2024 on the Operation of Digital Financial Asset Trading, Including Cryptoassets, as amended by OJK Regulation No. 23 of 2025.

Republic of Indonesia. (1847). Kitab Undang-Undang Hukum Perdata [Indonesian Civil Code] (Burgerlijk Wetboek, Staatsblad 1847 No. 23, as applicable).

Republic of Indonesia. (2008/2024). Law No. 11 of 2008 concerning Electronic Information and Transactions, as amended, most recently, by Law No. 1 of 2024.

Republic of Indonesia. (2019). Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions.